Statement of
Ronald E. Miller
Chief Information Officer
Federal Emergency Management Agency
Committee on Government Reform
Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations
Subcommittee for Technology and Procurement Policy
U.S. House of Representatives

May 2, 2002

Good morning, Mr. Chairman and Members of the Committee. I am pleased to be here today to talk about information technology security. Although I am not in a position to express the Administration's views on H.R. 3844, the 'Federal Information Security Reform Act of 2002,' or 'FISMA', I thought it would be useful to share FEMA's experience with the Subcommittee. I understand that FISMA would reauthorize and amend the Government Information Security Reform Act ("GISRA") and would like to share both my agency's experiences with GISRA and my perspective as the CIO Council's Security Liaison.

My testimony today will include topics in the following areas:

- FEMA's Approach to Information Technology ("IT") Security
    - Philosophy

    - Minimum Standards
    - Performance Goals
    - Capital Planning and Investment Process

- GISRA Experience
    - General Comments
    - What We Like Best

- FISMA Comments
    - General Comments
    - Potential Areas for Improvement

- Moving Forward
    - Strategic Directions

FEMA's Approach to Information Technology ("IT") Security

I would like to spend just a few moments describing FEMA's approach to IT security. Our approach to IT security strongly shapes our opinions concerning GISRA and the pending legislation known as FISMA.

FEMA's IT security philosophy is fairly straightforward. As a federal agency, we must deliver mandated services and products, and we must do so in full compliance with the laws of the land. What this means for us is that as we implement IT solutions to support our business processes, we must ensure that the IT solutions incorporate the security requirements put forth in public laws, Executive Branch directives, federal standards, and agency-specific policies.

We view the mentioned security requirements as providing the minimum security standards for our systems. A critical component of our process is ensuring that

all of our information systems meet a minimum set of standards. These standards are consistent with public laws and include:

- A formally certified system security plan
- Formal accreditation and approval to operate by the appropriate management official
- Tested contingency plans
- Implemented incident handling capabilities
- Security education awareness program
- Capital plan for funding security across the system's lifecycle

Our approach is to use a well-disciplined capital planning and investment process that ensures security costs are incorporated into the system development lifecycle. Our capital planning process is strongly linked to the agency's performance plan and goals. Using this approach, we have created a framework whereby IT solutions are implemented to support prioritized agency mission requirements and security is made a part of the IT solution itself. In this manner we are also able to demonstrate that the resources we apply to our IT security activities are directly in line with the agency's performance goals.

GISRA Experience

Overall, there are noticeable improvements being made across the Federal government in the area of IT security. GISRA has helped put management focus on this important problem. We still have need for additional progress, however, and FISMA is sound and will help.

The CIO community overall views GISRA as a very positive step forward for improving IT security in the federal government. GISRA codified many of the requirements put forth in OMB A-130. The codification of the A-130 requirements signaled a heightened awareness on the part of legislative branch

concerning the importance of implementing adequate IT security. The language in GISRA helped to clarify the role of the Chief Information Officer as being responsible for implementing an adequate IT security program across their agency. Also, GISRA required that each agency designate a senior official to head their IT security program and report to the Chief Information Officer.

An aspect of GISRA that we have found to be particularly useful is the annual report. The annual report is developed from program reviews conducted by the Chief Information Officer and combined with an independent assessment prepared by the agency's Inspector General. The development of the annual report is a significant undertaking and provides a significant benefit in terms of ensuring that the state of IT security is well documented and understood by senior agency managers.

FISMA Comments

In general, FEMA sees FISMA as similar to GISRA in most regards. Given the many similarities between FISMA and the existing GISRA we are confident in our abilities to implement FISMA, if enacted.

There are a number of areas in which, from the information security technologist's point of view, the bill needs improvement. For example, the bill should address the following:

- Stronger link between IT security requirements and the capital planning process
- Stronger emphasis and resources for IT security training
- Retention of IT security professionals
- Support for day-to-day security efforts
- Individual accountability for security

OMB has made it clear that IT capital investments must include consideration for implementing adequate IT security. Implementing adequate security requires having adequate resources. OMB's tying the approval of IT spending to a demonstrable security plan would provide a powerful incentive to program officials.

We do believe that in order to implement adequate security, the federal government requires a workforce that is well-trained and prepared to address the complex issues found in IT security. A strong emphasis should be placed on providing resources that provide training to employees responsible for implementing minimum federal standards. It would be very useful if the federal government provided IT security training in perhaps the same way that it offers standardized training in technology subjects, management skills, leadership development, and other professional disciplines.

Developing a well-trained federal workforce is important, but equally important will be our ability to retain this workforce. We support the Administration's Managerial Flexibility Act , which would allow federal agencies the flexibility to provide hiring and retention incentives to potential employees, including IT security professionals. This is particularly important when we consider that a significant portion of the current federal IT workforce will be eligible for retirement over the next 10 years.

There needs to be overarching support for the day-to-day security efforts across the Federal government. Examples include Carnegie Mellon CERT, FedCIRC (incident support), patch distribution services (just beginning at GSA), training, and guidelines (e.g., risk management). .

Finally, there is a strong need to hold federal government officials individually responsible in their performance plans for the implementation of security within their programs.. It has been demonstrated in numerous ways that employees

who have a personal stake in the success of a particular program will generally deliver a higher level of performance. A corresponding side to this is rewarding those employees that do deliver high levels of performance.

Moving Forward

In the future, there will be a need to coordinate with the Office of Homeland Security to leverage the federal government and link with other governmental and industry representatives to provide an effective cyber security capability.

The world has changed in many ways since September 11 last year. We are in a time of major changes in our approach to delivering emergency management services. It is very clear from the priorities expressed by OMB that electronic government is, and will continue to be, a major strategic direction for the federal government. The concept of electronic government will greatly change the manner in which we do business. To realize the full potential of electronic government, we must be able to implement electronic information sharing horizontally between government agencies, vertically from the federal government to the states, and very importantly, to the American public. An enabling factor will be our ability to implement and enjoy the benefits of electronic government, and do so in a manner whereby the risk does not outweigh those benefits.

Close

I am looking forward to working with this committee and each one of you in helping the federal government address needed improvements in federal IT security. Thank you for the opportunity to be here today. I will be happy to answer any questions you may have.